Abstract

The invention relates to a method for authenticating a smart card (*SIM*) in a messaging network, preferably a GSM network, wherein an optionally secret algorithm and a secret key are stored in a smart card (SIM), whereby for authentication the network or a network component first transfers a random number to the smart card, a response signal is generated in the smart card by means of the algorithm, the random number and the secret key, said signal being transmitted to the network or network component in order to check the authenticity of the card there. According to the invention both the secret key and the random number transferred by the network are split into at least two parts to form the authentication message, one part of the transferred random number and one or more parts of the secret key being encrypted by means of a one- or multistep, preferably symmetrical calculation algorithm. To output an authentication response, a selectable part of the encryption result is transferred to the network.

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 6 :
G07F 7/10

A1

(11) Internationale Veröffentlichungsnummer: WO 99/57689

(43) Internationales Veröffentlichungsdatum: 11. November 1999 (11.11.99)

(21) Internationales Aktenzeichen: PCT/EP99/02848

(22) Internationales Anmeldedatum: 27. April 1999 (27.04.99)

(30) Prioritätsdaten:
198 20 422.1 7. Mai 1998 (07.05.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: GIESECKE & DEVRIENT GMBH [DE/DE]; Prinzregentenstrasse 159, D–81677 München (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: VEDDER, Klaus [DE/DE]; Ainmillerstrasse 38, D–80801 München (DE).

(74) Anwalt: KLUNKER, SCHMITT–NILSON, HIRSCH; Winzererstrasse 106, D–80797 München (DE).

(81) Bestimmungsstaaten: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

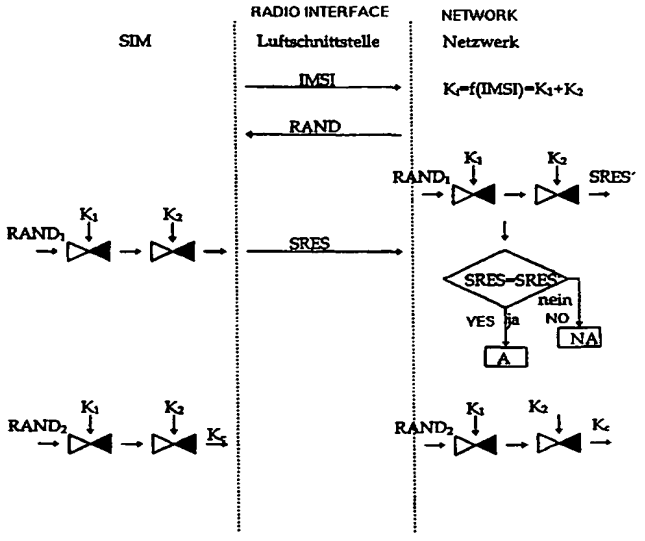
Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD FOR AUTHENTICATING A CHIP CARD IN A MESSAGE TRANSMISSION NETWORK

(54) Bezeichnung: VERFAHREN ZUR AUTHENTISIERUNG EINER CHIPKARTE INNERHALB EINES NACHRICHTENÜBERTRAGUNGS–NETZWERKS

(57) Abstract

The invention relates to a method for authenticating a chip card (SIM) in a network for transmitting messages, preferably in a GSM network. According to said method, an optionally secret algorithm and a secret key are stored in a chip card (SIM). In order to authenticate the card, the network or a network component first transmits a random number to the chip card. A reply signal is then generated in said chip card using the algorithm, the random number and the secret key, and transmitted to the network or network component where the authenticity of the card is checked. The authentication message is formed by dividing the secret key and the random number transmitted by the network into at least two parts each. A part of the transmitted random number and one or more parts of the secret key are encoded with a single or multi–stage, preferably symmetrical computation algorithm. A selected part of the product of the encoding procedure is transmitted to the network in order to issue an authentication reply.



(57) Zusammenfassung

Die Erfindung betrifft ein Verfahren zur Authentisierung einer Chipkarte (SIM) in einem Netzwerk zur Nachrichtenübertragung, vorzugsweise in einem GSM–Netzwerk, bei dem in einer Chipkarte (SIM) ein gegebenenfalls geheimer Algorithmus sowie ein geheimer Schlüssel gespeichert ist, wobei zur Authentisierung zunächst vom Netzwerk oder einer Netzwerkkomponente eine Zufallszahl an die Chipkarten übertragen wird, in der Chipkarte mittels des Algorithmus, der Zufallszahl und des geheimen Schlüssels ein Antwortsignal erzeugt wird, das an das Netzwerk bzw. die Netzwerkkomponente übermittelt wird, um dort die Authentizität der Karte zu überprüfen. Gemäß der Erfindung wird zur Bildung der Authentisierungsnachricht sowohl der geheime Schlüssel als auch die vom Netzwerk übertragene Zufallszahl in jeweils wenigstens zwei Teile aufgeteilt, wobei ein Teil der übertragenen Zufallszahl und ein oder mehrere Teile des geheimen Schlüssels mittels eines ein– oder mehrstufigen, vorzugsweise symmetrischen Berechnungsalgorithmus verschlüsselt werden. Zur Ausgabe einer Authentisierungsantwort wird ein auswählbarer Teil des Verschlüsselungsergebnisses an das Netzwerk übertragen.